

RECEIVED
CENTRAL FAX CENTER

OCT 19 2007

Application No. 10826475 (Docket: CNTR.2223)
37 CFR 1.111 Amendment dated 10/19/2007
Reply to Office Action of 10/17/2007

AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

SUMMARY OF THE INVENTION

[0020.1] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes a cryptographic instruction fetch logic and execution logic. The fetch logic is disposed within a microprocessor and is configured to receive a cryptographic instruction is received by a microprocessor as part of an instruction flow executing on the microprocessor. The cryptographic instruction prescribes one of the cryptographic operations, and also one of a plurality of cryptographic key sizes. The execution logic is disposed within the microprocessor and is operatively coupled to the cryptographic instruction. The execution logic executes the one of the cryptographic operations. The execution logic has a cryptographic key size controller that employs the one of a plurality of cryptographic key sizes during execution of the one of the cryptographic operations.

[0021] One aspect of the present invention contemplates an apparatus for performing cryptographic operations. The apparatus has a cryptography unit within a microprocessor and key size control logic. The cryptography unit executes one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes the one of the cryptographic operations. The cryptographic instruction is fetched from memory by fetch logic in the microprocessor. The cryptographic instruction also prescribes a key size to be employed when executing the one of the cryptographic operations. The key size control logic is operatively coupled within the cryptography unit. The key size control logic directs the device to employ the key size when performing the one of the cryptographic operations.

[0022] Another aspect of the present invention provides a method for performing cryptographic operations. The method includes, within a microprocessor, receiving

Application No. 10826475 (Docket: CNTR.2223)
37 CFR 1.111 Amendment dated 10/19/2007
Reply to Office Action of 10/17/2007

fetching a cryptographic instruction from memory that prescribes a prescribes cryptographic key size for employment during execution of one of a plurality of cryptographic operations; and within the microprocessor, executing the cryptographic instruction and employing the cryptographic key size when executing-performing the one of the cryptographic operations.